Tab D

Preliminary Research and Development Roadmap for Protecting and Assuring the Transportation Infrastructure*

* This document is one component of a longer report entitled *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures* (Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office. Washington, D.C. July 1998). For more information, please see <URL:http://www.ciao.gov/>.

Contents

Contents (Cont.)

Tables

Figure

Section 1
Introduction

This document charts a systematic course or "roadmap" (i.e., from fiscal year [FY] 1998 to about FY 2010),[1] for conducting public and private research and development (R&D) activities needed to enhance security and reduce vulnerabilities of the transportation infrastructure. This roadmap was developed by a study team of knowledgeable representatives from government, industry, academia, and institutes, and the national laboratories. Additional experts and contributors provided comments. These experts are listed in the Appendix.

1.1 Scope of the Infrastructure

The U.S. transportation infrastructure includes surface, air, and waterborne components. Vulnerabilities and security needs are discussed for (1) public and private airborne and surface aviation activity; (2) railway and highway movement and trans-shipment of goods and people, including intercity passenger and mass transit services; and inland waterborne commerce, maritime navigation, and port and terminal facilities. Other means of transport, such as oil, gas, and water transmission pipelines, are discussed in specific infrastructure assurance documents.

1.2 Characterization of the Infrastructure

The United States depends on transportation for most of our commerce and much of our success as a nation. The domestic transportation system offers a set of options for safe and reliable movement of freight and people. Both public and private entities own and control the components that provide these options. For example, the intercity freight rail system, its terminals, most of its rolling stock and interchange facilities, and its motive power are privately owned. Commercial airports, port facilities, inland and coastal waterways, and the highway and mass transit systems are either publicly owned or directly subject to public authority; the fleets that use these infrastructures (e.g., cars, trucks, buses, planes, ships) are, except for mass transit vehicles, privately owned. The air traffic control system and the navigation and positioning satellite constellation, which provide one or more vital services to most air and surface traffic, are owned and operated by the federal government.

Recognition of the need for safe and reliable transportation has stimulated competition (by both public and private agencies) to meet the demand for widespread, varied carrier capabilities. The transportation system has developed all-encompassing

[1] All years referenced in this document are fiscal years.

networks and services; that is, excess capacity for transporting freight and people. Although this capacity margin provides a resilient means for dealing with contingencies that can lead to short-term disruptions, it does not guarantee an expeditious, efficient response to catastrophic or major disruptions. For example, operation and control of much of the transportation system increasingly is becoming centralized to save costs and enhance the capability for real-time system monitoring at a single control point.

Centralized control has the potential to increase vulnerability because an attack could be catastrophic if it targeted a control center. Moreover, procedures and tools that permit knowledgeable authorities to deal effectively with security breaches and other localized disruptions by exercising independent judgment (i.e., "distributed processing") may be disappearing on key components of the overall system. Centralized command and control that intensely relies on electronic communications now is open to hostile, or accidental but pernicious, disruptions of, and intrusions into, the electronic message-passing system that enables such control (so-called "cyber events"). These events can disrupt overall operations more easily than a simple, physical attack, although a physical attack could be devastating if coordinated to target key "choke points."

1.3 Issues and Trends

The consistent, but flexible, U.S. transportation system has engendered site-specific specialization and mutual dependence across the entire nation. Unlike the frontier days, regions and communities of the present probably could not sustain themselves for extended periods because of their dependence on safe and reliable transportation and communication.

However, while the need for community, regional, and global connectedness has increased, actual physical links have declined in number and coverage, especially for smaller communities. Many communities have lost both rail freight and common carrier intercity passenger access in the past 40 years. Despite more freedom to enter the carrier market (because of a wave of transportation deregulation legislation), the number of rail, bus, and barge companies in the United States has declined during the 1990s. Only five domestically owned rail carriers of national stature remain.

Whereas railway service has decreased, roadway miles have increased, though at a slower pace than in the 1950s when construction of the Interstate highway system began. Nonetheless, because of the state of roadways and the number of substandard and unsafe bridges, the U.S. primary and secondary highway system is unsatisfactory in light of demands placed upon it. The gap between highway needs and highway performance is the greatest it has been in decades, primarily because of deferred spending and reduced maintenance budgets at the federal level and in most states. The Intermodal Surface Transportation Efficiency Act of 1991 has started to alleviate this situation by providing resources for road improvements and bridge replacements.

Because tax-supported mechanisms have not supported an increase in transportation capabilities formerly under public authority, including transit operations and major highway construction, the shift toward private commercial interests and joint public-private ventures is expected to continue. Thus, the primary responsibility for security of the affected infrastructures could shift to interests and organizations that may be poorly suited and positioned to handle such responsibility (compared to public security agencies operating under long-established arrangements). This development is especially worrisome because private organizations may not be able to justify increased security because of financial considerations and without public subsidies.

The desire to reduce costs and increase efficiency in the transportation infrastructure has increased our reliance on information technologies as substitutes for capital investment in physical capacity expansion and/or as a principal tool of strategic and system planning. To protect the transportation infrastructure from physical and cyber threats and vulnerabilities, experienced human surveillance is being displaced by automated surveillance. As a result, the security information is only as reliable and timely as the reliability and durability of the technology, which may not incorporate a “learning” component that, with human-provided security, is value added. Because much of the nation’s fixed transportation infrastructure is relatively isolated, reliability and durability are critical issues.

Section 2
Threats and Vulnerabilities

Many threats and vulnerabilities are direct consequences of emerging open architectures, which allow extensive information sharing and asset management, centralized control, and infrastructure isolation. The lack of a fully secure and reliable alternative to the space-based navigation system also is problematic. A wide variation in the perceived magnitude of the transportation system's vulnerability exists among key decision makers. In part, this situation may be a result of a potentially large gap between the theory and the practice of operating transportation systems as complete, yet often interdependent, networks, rather than as discrete point-to-point components. Concern has been expressed about the nature of actual security threats (physical and cyber) and management's understanding and ability to prepare for, and deal with, threats before they become catastrophic events. Recent events have shown that terrorists are willing and able to unleash chemical and biological agents in mass transit facilities; moreover, it cannot be ruled out that they are equally willing and able to attack air terminals, undertake large-scale cyber invasions, or wreak concerted destruction on multiple road and rail "choke points." Decision makers need to determine whether terrorists could be intercepted before an attack begins, and, if not, what mechanisms and capabilities could be counted on to detect the attack in a timely fashion and mitigate its consequences. Both physical and cyber threats need to be considered.

Most if not all of the R&D recommendations for assuring and protecting the transportation infrastructure fall into one of five general action areas:

- Awareness training for threats and vulnerabilities,
- Intrusion and attack prevention,
- Incident mitigation,
- Incident management, and
- Functional recovery.

Research is needed to reduce vulnerabilities in the transportation system and to mitigate their consequences. This research falls into one of four broad categories:

- Identification and Measurement of, and Awareness Training for, System Vulnerabilities;

- Development/Adaptation of Monitoring, Detection, Mitigation, and Incident Response Hardware;

- Development/Adaptation of Monitoring, Detection, Mitigation, and Incident Response Software; and

- Information Assurance, Human Factors, and Institutional Effects in Preparedness and Response.

For these activities, the goal is to substantially enhance capabilities within the five general action areas to reduce system vulnerability to an acceptable level, in particular on the vulnerabilities introduced by the following:

- Increasing openness of communication architectures;

- Increasing centralization of command and control functions at an ever-decreasing number of centers for rail network control, urban traffic management, and urban transit management; and

- Increasing importance and size of intermodal trans-shipment facilities, such as ports, rail classification yards, and truck terminals, which makes them more visible and likely targets.

Although some concern has been expressed about the security of air route traffic control centers (ARTCCs), generally "distributed processing" across regional and local control centers, with its flexibility to hand off control, has made these centers somewhat less vulnerable to physical attack. Moreover, the interface limitations of the admittedly antiquated computer systems used in ARTCCs have ironically, at least in the short term, significantly reduced their cyber vulnerability.

The Federal Aviation Administration (FAA), which continues to develop and install security measures for the ARTCC system, has implemented its own security R&D plan in the context of greater decentralization of responsibility. The final report of the White House Commission on Aviation Safety and Security, released in February 1997, contained the kernel of a recommended approach to aviation security R&D. Much of that approach supports and expands upon ongoing FAA research efforts, including explosive/weapons detection, human factors research, airport security, and aircraft protection through materials hardening.

With respect to emerging technologies for air and maritime navigation, the lack of secure redundancy for the positioning capabilities of the Global Positioning System (GPS) satellite constellation is considered to be a possible vulnerability, but no specific remedial actions in R&D have been identified. Supplementary systems (e.g., the Global Navigation Satellite System [GLONASS], LORAN-C, and ground-based radio-frequency [RF] pseudolites) exist and could be maintained, while alternatives to the C/A (coarse

acquisition) GPS transmission code, together with anti-jamming and message-encryption technologies, are becoming available.

One of the main goals of security R&D is to maximize the capability for complex systems, such as the physical and information infrastructure of transportation, to achieve a "soft landing" in the event of massive failure of some component. Another goal is to understand the role that human factors play in the prevention and effective remediation of such a failure. In particular, do individuals in critical command and control positions, from top to bottom of a decision chain, generally possess the kind and degree of sensitivity to low-probability events (such as terrorist attacks) necessary to effectively function in response to a detected threat or actual attack? Do they have the necessary knowledge and span of control? Are "person-machine interfaces" in transportation applications evolving to the point that both sides of this interface can be counted upon to perform successfully in critical situations?

Section 3
R&D Topics and Activities

The transportation infrastructure study team identified four general categories for key R&D tasks. The goal was to capture all of the individual and shared recommendations of team members in a systematic manner. Recommendations were compiled from knowledgeable outside individuals contacted by each team member, as well as by the team's collective understanding. These categories are as follows:

- *Identification and Measurement of, and Awareness Training for, System Vulnerabilities.* The overall purpose is to develop a suite of vulnerability assessment and simulation tools that can identify the existence and location of key weaknesses within systems and instruct those who need to know how to correct those weaknesses. Among the outputs of these methodological developments would be measures to quantify the comparative security of centralized and distributed network control schemes. It may be possible to adapt techniques used in military applications, but in the absence of supporting research, the suitability of such techniques is unknown.

- *Development/Adaptation of Monitoring, Detection, Mitigation, and Incident Response Hardware.* The replacement of experienced human monitoring and surveillance activity by automated technologies for monitoring and controlling systems imposes considerable pressure for real-time delivery of accurate, relevant, and reliable data from instruments designed to detect changes in the state of important system components. Similarly, the potential danger to human health and safety of direct intervention in the aftermath of incidents involving chemical/biological ("chem/bio") and other hazardous materials leads to a demand for remotely controlled damage investigation, assessment, and remediation equipment. It is doubtful that such equipment exists in applications readily transferable for specific use by the transportation infrastructure.

- *Development/Adaptation of Monitoring, Detection, Mitigation, and Incident Response Software.* This category echoes the concerns of the previous item, but with more direct reference to cyber attack rather than to physical attack.

- *Information Assurance, Human Factors, and Institutional Effects in Preparedness and Response.* It is important that transportation systems conduct operations in a manner that does not unnecessarily increase risk, even in normal operation. Therefore, assurance of the reliability and accuracy of electronic information received on a regular, continuous basis is critical. Research can help to define and establish "fail-safe" mechanisms for maintaining this assurance. Systems still may become unstable; however, when they do or when untoward events occur, a more complete

understanding is essential, through advanced research, of human response to such conditions and how negative manifestations can be neutralized.

Research topics within each of these four areas are presented in Table D-1. The table indicates the type of research needed, and validation of the principal goals of and challenges to successful accomplishment of the research, targeted infrastructure vulnerabilities, and level of importance/priority. Assigning priority creates the recommended hierarchy for allocating limited funding resources. Sections 3.1–3.4 provide more detailed descriptions of each topic within the research categories.

3.1 Identification and Measurement of and Awareness Training for System Vulnerabilities

3.1.1 Vulnerability Analysis of Existing Systems

Description

This analysis would consist of a broadly encompassing investigation into the status of existing vulnerabilities within and between operating modes. Special emphasis is given to situations in which communications architectures are generally open, and a distributed/decentralized command and control system is not a management philosophy. Pilot studies of actual operations would be performed (with concurrence of management); buy-in and adoption (with peer review); development (with validation); and application of appropriate simulation, gaming, and optimization measures.

A representative panel, consisting of elected and appointed technical decision-makers, would serve as an ongoing advisory committee for project oversight and guidance. The objective is to weigh the susceptibilities and instabilities possibly inherent in existing systems against the potentially greater operating costs and reaction times of closed architectures and/or distributed control. A model or set of models may need to be tailored specifically for application to three to five prototypical structures in transport operations. The U.S. Department of Defense (DoD) and Federal Emergency Management Agency Consequences Assessment Tool Set can provide a workable departure for developing and applying a consolidated tool.

Goals and Challenges

The objective of applied research is to identify (for up to five typical organization types across transportation modal operations) significant vulnerabilities that can exist as a function of the communications architecture and/or control system in place. Should such vulnerabilities be identified, it still could be difficult to get operating entities to consider a serious restructuring instead of an alternative, less vulnerable, but possibly more stable (and costly) architecture or control structure. Several research teams would need to work from three to five years to identify and build the appropriate tools, even with all stakeholders participating in the process.

Table D.1 Summary of Research Topics by Category

Research Topic					
No.	Title (Type[a])	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category[b]
Identification and Measurement of and Awareness Training for System Vulnerabilities					
1	Vulnerability Analysis of Existing Systems (A)	Information, policy guidance	Conduct pilot studies to get to the root of the issue and to obtain "buy-in" from private operators	Complexity	Most important
2	Simulation Tool Development: (B, A, ATD)	Software and training packages for "what if" situations.	Identify and capture relevant contingencies to include in each system simulation structure; generate appropriate and comprehensive input data for conducting analyses impartially; automate decision support; maximize productivity of infra-structure investment; assure continuity; understand trade-offs.	Physical, cyber, interdependencies	Very important
3	Determination of Risk Perception of Transport System Managers (B, A)	Information and training	Identify key characteristics at all appropriate decision levels; quantify important parameters.	Physical, cyber, interdependencies	Very important
4	Communication and Inculcation of Sound Risk Management Principles (ATD, POP)	Information and training	Develop comprehensible language and terms for transmitting useful knowledge; use effective communication methods.	Complexity, cyber, interdependencies	Very important
5	Capacity Margin Analysis (A)	Information, policy guidance	Quantify avoided contingency losses in net benefit calculations.	Complexity, interdependencies	Important
6	Emergency Communications (A)	Information, policy guidance	Acknowledge that practices and systems differ across modes and infrastructures.	Interdependencies	Very important

Table D.1 (Cont.)

Research Topic No.	Title (Type[a])	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category[b]
Development/Adaptation of Monitoring, Detection, Mitigation, and Incident Response Hardware					
7	Real-time Hazard Threat and Detection Monitoring (B, A, ATD, POP)	Instruments, algorithms, diagnostics	Increase or adapt capability to detect/ classify physical/cyber threats and component failure cost-effectively and expeditiously; add new capabilities.	Complexities, physical, cyber	Most important
8	Robotics Development and Adaptation (B, A)	Hardware (robots, servo-mechanisms), instruments	Protect responders; assist victims; expedite recovery; assist in surveillance and remote detection.	Physical, cyber	Very important
9	Improvement of In-use Performance and Replacement Functionality of Transportation Structures (A, POP)	Lightweight, portable com-ponent application and replacement structures	Match advanced materials with specific structural replacement needs; develop efficient, longevity-producing features for physical infrastructure.	Physical	Very important
10	Unified Vehicle Guideway Systems (Hardening) (A)	Improved equip-ment, structures, materials	Link to threat identification technologies and advances in materials science.	Physical	Very important
Development/Adaptation of Monitoring, Detection, Mitigation, and Incident Response Software					
11	Asset Management (A, ATD)	Software for case analyses; hardware/ integrated software for flaw detection	Add reliability and utility to decision makers.	Physical	Very important
12	System Representation Improvement (ATD, POP)	Comprehensive databases for threat management, incident prevention, and multiple system response	Maximize amount of data on relevant subjects that can be clearly collated for rapid comprehension.	Physical, cyber	Very important
13	Intrusion Detection: Adaptation and Custom Development (ATD, POP)	Software	Selectively adapt and apply NASA, DOE, USCG, and DoD tools to transportation systems.	Physical, cyber	Most important
14	Cyber Vulnerability Data Warehouse (ATD, POP)	Clearinghouse for all cyber vulnera-bilities affecting transportation systems	Construct models of transportation computer systems and compre-hensive configurations data center.	Cyber	Important

Table D.1 (Cont.)

Research Topic No.	Title (Type[a])	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category[b]
Development/Adaptation of Monitoring, Detection, Mitigation, and Incident Response Software (Cont.)					
15	Threat/Intelligence Database and Network (potentially under DOJ/FBI leadership) (ATD, POP)	Clearinghouse for all threats related to transportation systems; real-time intelligence for response and law enforcement	Coordinate with FBI National Infrastructure Protection Center to develop all relevant information.	Physical, cyber interdependencies	Most important
Information Assurance, Human Factors, and Institutional Effects in Preparedness and Response					
16	Information Assurance (A, ATD)	Advanced, integrated software systems with high level of AI	Apply random encryption and AI techniques to assure message continuity and integrity.	Cyber, interdependencies	Most important
17	Software Assurance (A, ATD)	Software with advanced fault checking and self-diagnosis	Assure nondegrading, reliable performance of network control software.	Interdependencies	Most important
18	Human Factors Analysis (A)	Information and training	Characterize the problem and seek a solution, not the reverse.	Complexity, physical	Most important
19	Recovery Training (A)	"Triage" education; training with optimization tools developed in vulnerability analysis of existing systems	Apply developments in dynamic traffic assignment in these situations.	Interdependencies	Important
20	Computer Emergency Response and Emergency Response and Recovery Assessment Capacity Building (B, A, POP)	Information	Maintain study resources in "standby" mode, for rapid deployment when needed.	Physical	Very important
21	Public Infrastructure/Private Security (POP)	Information	DOT has committed to support this objective with research on optimal deployment of capability.	Complexity, interdependencies	Most important

[a] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

[b] The order of the R&D topics within a priority category (i.e., most important, very important, important) does not imply relative importance.

Rationale for the Research and Desired Results

This research targets awareness training, but it also can pertain to informing policy development.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would conduct pilot studies of actual transportation operations. Funding required for these efforts is estimated to be $9 million. Before 2005, research activities would include developing assessment tools, completing peer review, and validating specific tools. Funding required for this effort is estimated to be $9 million. Before 2010, researchers would complete their assessments of the transportation system. The cost for this work is estimated to be $6 million.

3.1.2 Simulation Tool Development

Description

Among all of the vulnerability assessment tools that can be developed, implemented, and communicated to decision makers, none are more important than simulation and gaming. Both applied (possibly adaptational) and developmental research are needed to build and tailor software and training packages for "what if" situations, covering inter- and intrametropolitan operations for each of the major means of transportation — air, highway, rail, waterway, and intermodal combinations.

Knowledge of, and sensitivity to, control structures within all operations are required to develop sufficiently comprehensive, effective software. The transportation system must operate as a complex network, not as a set of simple point-to-point connectivities. To meet this goal, it is essential that operations personnel and decision makers accurately simulate and understand the network dynamics. Basic (to extend network theory) and applied (to apply to specific conditions) research are needed to understand the principles and guidelines that govern the construction of software and training packages for network management within and across modes. Flexibility within the modeling structures should make it possible to explore the effects of new control hierarchies.

Modeling tools would be validated for each mode and applicable control structures. Thus, their development must be accompanied and shaped by real-world exercises, including compiling existing physical inventories of the total transportation infrastructure, analyzing representative sample pieces of the individual systems, evaluating intersystem connectivity nodes, and identifying all physical and cyber choke points. Pilot studies are essential during the early stages of development.

Goals and Challenges

The goals of these R&D efforts are to identify and capture all relevant contingencies to include in the simulation structure for each system, to generate appropriate and comprehensive input data for analyses, and to identify the conditions under which analyses can be conducted impartially. Selecting and correctly programming the appropriate probability constructs for reliable simulation (e.g., Monte Carlo, Bayesian/Markovian, "chaos," or hybrid methods) are a significant challenge. The goal is to develop tools that (a) assure continuity of operations, (b) contribute to automated decision support, (c) maximize the productivity of the existing infrastructure to help guide investment decisions, and (d) show clearly that unavoidable trade-offs exist among productivity, service reliability, and preparation for rare events.

Rationale for the Research and Desired Results

This research targets awareness training for threats and vulnerabilities, one of the five essential action areas identified above. It could lead to the identification and remediation of existing infrastructure vulnerabilities and to the prevention or mitigation of new threats; it also could help to optimize the overall use of transportation resources and increase preparedness of system operators. More generally, although strictly within the context of infrastructure security, it could help to assure continuity of operations, contribute to automated decision support, maximize productivity of the existing infrastructure, help to guide investment decisions, and show clearly the unavoidable trade-offs that exist among productivity, service reliability, and preparation for rare events.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would identify and evaluate ways to create tools that can be used to predict and manage events. Funding required for these efforts is estimated to be $15 million. Before 2005, research activities would include developing and validating the basic tools created in the near-term research. Funding required for this effort is estimated to be $15 million. Before 2010, researchers would validate and deploy the completed set of tools. The cost for this work is estimated to be $5 million.

3.1.3 Determination of Risk Perception of Transport System Managers

Description

A systematic effort to understand and formalize awareness and perception of the risks inherent in current transport operations is necessary for building components of the simulation tools. Through basic research, analysts would characterize and quantify the elements of these structures, while through applied research, they would explore the use

of this systematic characterization within each mode and control hierarchy of the transportation infrastructure.

Goals and Challenges

Researchers would identify and develop quantitative measures of the key characteristics of risk perception at all appropriate decision levels. Again, conducting one or more initial pilot studies in a real-world operational context is essential so that private-sector managers understand and accept the merits of the research objective and its value to them.

Rationale for the Research and Desired Results

This research targets awareness training for threats and vulnerabilities and intrusion and attack prevention. A basic understanding is necessary for constructing simulation tools to identify and remedy infrastructure vulnerabilities and prevent new threats.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would conduct scoping activities. Funding required for these efforts is estimated to be $2 million. Before 2005, researchers would complete the analyses and have operating training in place for all functions. Funding required for this effort is estimated to be $2 million. Before 2010, researchers would identify and implement fully secure emergency response communications.

3.1.4 Communication and Inculcation of Sound Risk Management Principles

Description

Operators would have an information and training package about risk as a result of research described above (Section 3.1.3). Training, however, also is needed at all levels, not just for key decision makers, but to inculcate a “security awareness culture” across operating entities. The best means to provide this training and successfully communicate its message varies by worker task, scope of responsibility, and level of education.

Training can be conducted from remote locations via, for example, computer platforms (using CD-ROM) or the Internet. Thus, recent developments in distance learning and training should be considered. The result of applied research in this area is the development of systematic training tools appropriate for each mode and control hierarchy; actual implementation, however, would require field-testing and updating of each package. Implementation would include conducting a case study of adoption and use of formal risk management procedures by at least one operating entity for each physical

distribution mode. Proof of principle would demonstrate the effectiveness of risk management principles. Training also should cover security management/acquisition for managers, network security, security administration for system administrators, forensic analysis, and security testing and certification.

Goals and Challenges

This research effort is aimed at developing language and terminologies for knowledge transmission that are useful and comprehensible at all appropriate levels. The goal is to convince officials in the transportation sector, lawmakers, and others with vested interests that vulnerability management is necessary for normal daily operation and that it has a potentially high payoff.

Rationale for the Research and Desired Results

This research targets awareness training for threats and vulnerabilities, intrusion and attack prevention, and incident management. Development of a training program should incorporate the accepted cycle of identifying requirement analyses (e.g., task, organization, person within each structure) with task-based determination of the associated knowledge, skill, and abilities (KSAs) followed by instructional objectives tailored to instill each set of KSAs. It is necessary to communicate the true magnitude and type of risk to operating authorities so that they can identify and remedy infrastructure vulnerabilities, prevent new threats, and institutionalize the results of analyses conducted under Sections 3.1.1–3.1.3.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would develop a training program that would consider providing training from remote locations, such as computer platforms or the Internet. Funding required for these efforts is estimated to be $2 million. Before 2005, researchers would complete analyses and have training in place and operable. Funding required for this effort is estimated to be $2 million. Before 2010, researchers would identify and implement fully secure emergency response communications.

3.1.5 Capacity Margin Analysis

Description

Although “excess” infrastructure in the transportation system may not be an economically productive asset to owners, it may be essential to the protection of broader national interests with regard to total carrying capacity and security. In this case, the obligation to maintain a surplus capacity margin may more appropriately reside with the entire nation (i.e., taxpayers). Applied economic research at a high level of sophistication is needed to fully compute the costs and benefits of, and to guide national policy about, retaining capacity margin in (at a minimum) the rail freight, mass transit, and inland

waterway systems. The effort is a logical follow-on to Section 3.1.2 and concomitant to Section 3.1.1.

Goals and Challenges

This research seeks an accurate quantification of the losses from contingencies expected to arise in the absence of surplus capacity (i.e., avoidance of these losses would be the chief net benefit).

Rationale for the Research and Desired Results

This research is targeted at incident mitigation and incident management. Because rail carriers, to cite a specific situation, are now actively eliminating "excess" capacity, waiting until well into the next century to begin this investigation could result in the loss of potentially critical links in the infrastructure.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would develop a training program that would consider receiving training from remote locations, such as computer platforms or the Internet. Funding required for these efforts is estimated to be $2 million. Before 2005, researchers would complete analyses and have an operating training program in place. Funding required for this effort is estimated to be $2 million. Before 2010, researchers would identify and implement fully secure emergency response communications.

3.1.6 Emergency Communications

Description

Vulnerability can be an issue before and after an incident. Specifically, the emergency communications system that must support mitigation and management actions in the aftermath of an event can be vulnerable to sabotage or misuse. Applied research is needed to identify and develop the best means for securing communications systems channels.

Goals and Challenges

The need for security cuts across all critical infrastructures, but a "one size fits all" set of solutions may not exist. This project would identify the solutions most appropriate for responses to disruptions of transportation infrastructure to enable development and deployment of adequate systems.

Rationale for the Research and Desired Results

Research targets incident mitigation, incident management, and functional recovery, but it also can be related to protection from intrusion and attack if "fail-safe" communications systems are discovered. This project gives a needed head start to product development for fully functional and secure emergency response communications.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would identify and implement a fully secure emergency response communications function. Funding required for these efforts is estimated to be $6 million. Before 2005, this technology would be commercialized. Funding required for this effort is estimated to be $2 million.

3.2 Development/Adaptation of Monitoring, Detection, Mitigation, and Incident Response Hardware

3.2.1 Real-time Hazard, Threat, and Detection Monitoring

Description

Transportation's special needs for dealing with physical and cyber threats and detection monitoring equipment are associated with the isolation and scale of much of the infrastructure, the openness of public access to potentially vulnerable spaces (e.g., transit stations, garages), the reliance of most operating systems on the accuracy of electronic data, the overall visibility of structures (i.e., high public profile), and the demonstrated willingness of physical and cyber offenders to attack. This vulnerability is especially critical in the chem/bio area and in malicious computer "hacking" threats.

Component failure or impending failure needs to be avoided to ensure uninterrupted control of systems; however, means for detecting impending failure at remote sites are in their infancy with respect to the number and complexity of parameters monitored. High-resolution broadband applications, a possible solution to this problem, are not widely used for (or adapted to) transportation systems. Because many sites and structures need detectors across the physical and electronic dimensions of the transportation system, the cost of such detectors must decrease before an effective deployment can occur.

Goals and Challenges

Even if the unit cost of reliable detectors and monitors decreases substantially, the number required to cover the entire transportation network in fixed distributed configurations may still be prohibitively large unless a supporting logistics analysis can identify cost-effective placement strategies. Thus, both cost-reduction advancements and logistics analyses are needed.

Rationale for the Research and Desired Results

This research targets physical and cyber *intrusion detection*, attack and failure prevention, and *incident management* for scenarios that have either produced incidents or amply demonstrated feasibility. Thus, it is highly probable that this technology will not be available within the next 2–10 years.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would ensure that applied R&D is under contract. Initial development of detection devices would be under way. Funding required for these efforts is estimated to be $8 million. Before 2005, researchers would complete the prototype testing of the detection devices in six to eight parallel studies. Funding required for this effort is estimated to be $12 million. Increases in system capability and flexibility would continue through public-private partnerships. Before 2010, researchers would be in a position to commercialize the public-private ventures. The cost for this work is estimated to be $12 million.

3.2.2 Robotics Development and Adaptation

Description

In the aftermath of a physical attack, especially in large, semipublic spaces (e.g., terminals, transit centers), it may be hazardous for responders to intervene directly at or near the site. Applied research and some basic research are needed to identify and develop robotic technologies and remotely controlled servo modules capable of assessing damage, which usually is done by first responders. As a first step, existing DoD technologies should be investigated to determine if they are adaptable for this purpose.

Goals and Challenges

There is a need to tailor and deploy applications that can protect responders, assist victims, and expedite recovery without significant delay. The most effective means of assuring such deployment is to conduct pilot studies early in the project (i.e., involve highly likely locations, such as mass transit stations). Test scenarios for such a pilot study should be constructed pursuant to information collected for Transit Cooperative Research Program Synthesis Report No. 27, *Emergency Preparedness for Transit Terrorism* (Transportation Research Board 1997).

Rationale for the Research and Desired Results

This research targets incident management and, to a lesser degree, functional recovery to provide a required comprehensiveness of response and real-time remediation capability not currently available for many attack scenarios.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would develop and adapt robotic technology for remotely controlled modules to be used in situations in which first responders face dangerous hazards. Funding required for these efforts is estimated to be $5 million. Before 2005, researchers would complete the prototype testing of the remotely controlled modules. Funding required for this effort is estimated to be $7 million. Before 2010, researchers would be in a position to commercialize public-private ventures.

3.2.3 Improvement of In-use Performance and Replacement Functionality of Transportation Structures

Description

In the aftermath of physical attack, especially involving geographically isolated, but important, load-bearing structures (e.g., bridges, trestles, tunnels), it may be critical to bring the severed distribution link back into service in a fraction of the time normally required to provide temporary repairs. Strategic, simultaneous removal of key structures at multiple interchanges or at places where essential road and rail links are proximate could trigger a dangerous, if short-term, disruption of national commodity flow. Applied research with proof of principle is needed to understand the strength and durability of advanced, inexpensive, lightweight materials to provide modularity, portability, and performance safety for the various infrastructures. These attributes are currently not available except possibly for military application.

It is also important to understand performance safety of various infrastructures currently in place. As a first step, the adaptability of existing DoD technologies, as well as those of other agencies and organizations for which deployment of temporary structures is integral to their mission, would be investigated. In conjunction with this research, it also would be prudent to perform logistics analyses to define the optimal positions for stationing outage-response teams and materials. A broader, longer-term goal of this effort, in the context of recovery from incidents, would be to assemble a comprehensive disaster-recovery manual of practice. Such a manual also would be developed in conjunction with the computer emergency response topic discussed in Section 3.4.5.

Goals and Challenges

Advanced materials need to be matched with specific structural replacement requirements across multiple modes and missions. Reliable longevity of assets in place and their ability to withstand and mitigate physical attack are equally important objectives. In addition, structural modules would be located so as to minimize the total deployment time to locations where links are severed.

Rationale for the Research and Desired Results

The research targets functional recovery, which is clearly hampered by delays in restoring service to critical physical links. Functional durability (i.e., mitigation, recovery) is also targeted, but not all needs are known.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would develop and adapt materials to maximize modularity, portability, and /or durability of the function of permanent and temporary structures within the transportation system. Funding required for these efforts is estimated to be $5 million. Before 2005, researchers would complete field testing of up to five applications. Funding required for this effort is estimated to be $7 million. Before 2010, the goal would be to commercialize these structures.

3.2.4 Unified Vehicle/Guideway Systems (Hardening)

Description

Advances in transportation technology, especially in intelligent transportation systems (ITSs), automated highway systems (AHSs), and magnetic levitation, would increase the integration of vehicles and the guideways on which they travel (the so-called "intelligent vehicle infrastructure"). Such integrated systems could become more vulnerable to both physical and cyber attack, but preservation of their structural integrity would be essential to their protection in both senses. To that end, surface transportation experts need to enhance the blast resistance of aircraft (possibly by reviewing R&D plans from the Federal Aviation Administration). They also need to conduct applied research in damage-tolerant design for fixed guideways and other fixed structures.

Goals and Challenges

The specific threats for which the need exists (the threats would differ among modes and applications) must be identified. Advances in materials technologies need to be linked to a systematic improvement in guideway system equipment and structural durability.

Rationale for the Research and Desired Results

This research targets incident mitigation with respect to transport concepts emerging as actual hardware, but for which many risks are currently unknown and need to be anticipated.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would plan to complete scoping studies of materials technology needed to improve the durability and resistance to damage from physical and cyber attacks on transportation systems. Funding required for these efforts is estimated to be $2 million. Before 2005, researchers would develop prototypes to improve the durability of transport systems. Funding required for this effort is estimated to be $7 million. Before 2010, the goal would be to commercialize this technology.

3.3 Development/Adaptation of Monitoring, Detection, Mitigation, and Incident Response Software

3.3.1 Asset Management

Description

In a broader context than that of security maintenance, operating executives need to be able to manage network-configured physical and cyber assets in the most productive manner possible to maintain competitiveness and use passenger- and freight-carrying equipment in the best way possible. Understanding and instituting these principles would provide the foundation for successful security assurance structures.

Goals and Challenges

The capability for quantitatively defining and identifying the most efficient use of resources is not uniform across all transportation modes and not well demonstrated in the field. Development is continuing in flaw detection hardware and software. Appropriate decision analysis support tools also are in the development stage. This research spans all action areas.

Rationale for the Research and Desired Results

Specially tailored hardware and software needs cannot be met at the current level of operation-specific knowledge.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would conduct scoping studies of how to make the most efficient use of physical and cyber resources. Funding required for these efforts is estimated to be $1 million. Before 2005, researchers would validate and peer review prototype tools for decision analysis support. Funding required for this effort is estimated to be $2 million. Before 2010, the goal would be to commercialize this technology. Funding required for this effort is estimated to be $1 million.

3.3.2 System Representation Improvement

Description

One way or another, formatted data applications cut across all research categories in this document. Because such data are stored and processed through electronic media, database development needs are included here. Data are now available in both publicly accessible and privately controlled media, but only a fraction of the content has been systematically collated to enhance and inform emergency response. Much more data may need to be collected and usefully transcribed to an accessible visual medium — for example, geographic information systems (GISs). These data structures are critical to a more thorough understanding of physical vulnerabilities in the transportation infrastructure.

This topic is tied closely with infrastructure management because the representational capability envisioned involves the entire process, not simply the overlying (and underlying) physical phenomena. Thus, the comprehensible representation of data on system performance (e.g., capacity, speed, cost, connections, restrictions, ownership) is as important as, or equal to, that on location and configuration of public and private distribution channels and other hardware. Successful translation and adaptation of data on comprehensive system process characteristics would be the signal contribution of this undertaking.

Goals and Challenges

Researchers would maximize the amount of useful data that can be collated into clear, comprehensible formats for visual display in a manner that improves the understanding of interconnected and dependent systems and enhances the real-time, in-situ capabilities of incident responders and managers. A pilot study with direct private-sector participation and public-private interactions is essential to the ultimate acceptance of research results. Such a study would influence database development at an early stage by populating the data of series with systems data of direct relevance to the needs of ultimate end users.

Rationale for the Research and Desired Results

Technology development and proof of principle would be targeted at all action areas, but especially at awareness training, incident mitigation, and incident management. The technology and many of the capabilities exist; the challenge is to adapt and adopt them to these action areas in the most useful and complete manner.

Timeframe and Resource Requirements

In the near term (before 2002), requirements would be defined and development contracts awarded to at least two teams by the end of 2000. Methods for managing

transport system data in a clear format would be improved. Funding required for these efforts is estimated to be $20 million. Before 2005, in addition to integrating the database, researchers would complete testing and validation of a regional prototype suite of tools. Funding required for this effort is estimated to be $30 million. Before 2010, researchers would implement multiple applications, with full U.S. coverage assumed. Funding required for this effort is estimated to be $20 million.

3.3.3 Intrusion Detection

Description

On-line software (such as a real-time firewall) is needed to detect and automatically invoke countermeasures to cyber intrusions in day-to-day electronic transaction and control processes. The ability of this technology to forecast and detect such incursions, for nonmilitary applications, is generally in its infancy. Because of the significant quantity and diversity of electronic data interchanges that occur across transportation operations on a daily basis, this sector is vulnerable. Pilot studies, in particular with transportation clients, are strongly recommended.

Goals and Challenges

Researchers should adapt current capabilities in this area, including Computer Emergency Response Teams and incident response activities under development by DoD, the National Aeronautic and Space Administration, the U.S. Department of Energy, and others. Adaptation would occur first in transport operation data flow systems and then in identification and completion of knowledge and performance gaps. Direct integration with the U.S. Coast Guard's Computer Incident Response Team is a possibility.

Rationale for the Research and Desired Results

Technology development and proof of principle would target intrusion and attack prevention. It is believed that the technology and many of the capabilities exist; the challenge is to adapt and adopt them to these action areas in the most useful and complete manner.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would define requirements and award contracts to customize intrusion detection systems for the transportation infrastructure. Funding required for these efforts is estimated to be $4 million. Before 2005, researchers would complete the design and testing of systems and begin to implement multiple applications. Funding required for this effort is estimated to be $6 million. Before 2010, intrusion detection for physical and cyber assets would be commercialized. Funding required for this effort is estimated to be $1 million.

3.3.4 Cyber Vulnerability Data Warehouse

Description

Because of the diversity of computer systems and networks used throughout the transportation sector, models of their functions and interdependencies need to be constructed. Moreover, a comprehensive database of known cyber vulnerabilities specific to these systems needs to be developed. Both objectives could be served by establishing a data vulnerability clearinghouse, possibly modeled after one at Carnegie-Mellon University. This clearinghouse would contain the details of hardware, software, and communication components of existing and emerging systems. Through this mechanism, owners of vulnerable data repositories and networks could be notified early of a potential cyber incursion, as well as have a real-time channel to the latest information on firewalls and other security practices.

Goals and Challenges

Development teams must craft within a single facility a combined reference and proactive response capability that meet a wide variety of computer support and security needs across all transportation operations.

Rationale for the Research and Desired Results

Proof of principle would target intrusion and attack prevention. It is believed that the technology and many of the capabilities exist; the challenge is to adopt them, while adapting them to these action areas in the most useful and complete manner.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would define requirements and award contracts for an integrated facility that would provide intelligence concerning physical and cyber threats to the transportation system. Funding required for these efforts is estimated to be $1 million. Before 2005, researchers would complete a fully functional facility. Funding required for this effort is estimated to be $1 million.

3.3.5 Threat/Intelligence Database and Network

Description

The function described here would be closely integrated with that described in Section 3.3.4 (Cyber Vulnerability Data Warehouse). However, the emphasis would be on developing and disseminating intelligence in regard to specific terrorist plots for destroying physical infrastructure and malicious hacking (computer terrorism) directed at transportation functions. Activities could be modeled on, and directly coordinated with, those of the National Infrastructure Protection Center to be operated by the Federal

Bureau of Investigation (FBI). This topic and the cyber vulnerability data warehouse topic could be consolidated if an interagency agreement was drafted to create a comprehensive clearinghouse under the aegis of a Transportation Infrastructure Protection Threat Analysis Center.

Goals and Challenges

Early warning information and intelligence channels exist, especially for mass transit and aircraft operations. Proof of principle requires broadening and examining the scope in depth to embrace all transportation infrastructures. An office of the U.S. Department of Justice or the FBI probably would lead the networking effort to develop data, supported by multiple public- and private-sector organizations.

Rationale for the Research and Desired Results

Proof of principle and validation target intrusion and attack prevention. It is believed that many of the necessary capabilities exist. The challenge is to adopt them, while adapting them to these action areas in the most useful and complete manner.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would define requirements and award contracts for an integrated facility for providing intelligence in regard to threats. Funding required for these efforts is estimated to be $1 million. Before 2005, researchers would complete a fully functional clearinghouse. Funding required for this effort is estimated to be $2 million.

3.4 Information Assurance, Human Factors, and Institutional Effects in Preparedness and Response

3.4.1 Information Assurance

Description

Artificial-intelligence (AI)-based technologies can be used to ensure that a near-zero probability exists that electronic information and data flows that are degrading or corrupted (because of component failure or instability) would not be detected. Message encryption techniques are more sophisticated and able to thwart most hostile interception and decoding efforts. These capabilities are needed in the transportation infrastructure, but additional research could be required to define the most suitable approach for specific applications.

Goals and Challenges

Researchers would adapt information security capabilities available from DoD and other lead federal agencies to transportation data flow systems. Once these capabilities are adapted for the transportation infrastructure, researchers would identify and fill knowledge and performance gaps.

Rationale for the Research and Desired Results

Applied technology development is needed to support incident mitigation in a cyber context. Many of the capabilities exist: the challenge is to adopt these capabilities while adapting them to transportation operations in the most useful and complete manner.

Timeframe and Resource Requirements

In the near term (before 2000), requirements should be defined and utilization of existing tools well advanced. Funding required for this effort is estimated to be $2 million. Before 2005, design and testing should be completed, and tools should be ready for field implementation. Funding required for this effort is estimated to be $3 million. Before 2010, the AI-based technologies would be implemented and commercialized at an estimated cost of $1 million.

3.4.2 Software Assurance

Description

Artificial-intelligence-based technologies can limit to near zero the probability that purpose-based software installed in critical day-to-day information handling systems would deteriorate without detection and remedy. Further development of on-line fault checking and self-diagnostic capability of software is needed.

Goals and Challenges

The continuous, reliable performance of network control-related software, whatever the nature of the operational command and control structure, must be ensured, and there must be no degradation without diagnosis.

Rationale for the Research and Desired Results

Applied research and technology development is needed to support cyber incident detection and mitigation. Some operational needs may not be met by existing capabilities.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would define requirements and use existing tools to develop AI-based technologies to ensure, to the degree possible, the security of electronic information and data flows. Funding required for these efforts is estimated to be $2 million. Before 2005, researchers would complete the design and testing of these new tools. Funding required for this effort is estimated to be $3 million. Before 2010, AI-based technologies would be implemented and commercialized. Funding required for this effort is estimated to be $1 million.

3.4.3 Human Factors Analysis

Description

Humans always must be "in the loop" in all efforts to minimize (1) vulnerabilities, through predicting and evading dangerous physical and cyber incidents, and (2) negative consequences when such incidents occur. For the transportation infrastructure, it is important to know if experience has shown that the human role is uniformly beneficial (especially if fully automated alternatives exist). If the human role is not totally beneficial, researchers need to determine what training, education, and sensitivity conditioning would increase the likelihood of beneficial human intervention.

Goals and Challenges

Researchers must characterize actual problems and limitations in event prediction and response that are specifically attributable to human factors so that solutions to these shortcomings can be found. Conversely, they need to avoid bringing canned theories into play in search of human factor remediation "needs" (i.e., to discover rather than to apply).

Rationale for the Research and Desired Results

Applied research is needed to support all five action areas, but especially vulnerability assessment, incident mitigation, and incident management. A major effort is needed to develop information packages and training programs for operating authorities. A newly developed training regimen would incorporate the accepted cycle of identifying requirement analyses (e.g., task, organization, person within each structure), with task-based determination of the associated knowledge, skill, and abilities (KSAs). These steps would then be followed by instructional objectives tailored to instill each set of KSAs.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would characterize problems and limitations inherent in human preparedness, prediction, and response. Funding required for this effort is estimated to be $6 million. Before 2005, researchers would fully identify

and implement changes for preparedness and prediction. Funding required for this effort is estimated to be $4 million.

3.4.4 Recovery Training

Description

Understanding of "triage" decision processes and other essentials of emergency management is not normally incorporated into the training of individuals for high levels of control responsibility in transportation operations. The best techniques and principles for communicating such understanding have not been identified. The optimization tools developed under Category 1 projects should be incorporated into a training and awareness program tailored to each mode of operation and control organizational structure.

Goals and Challenges

Many recent methodological advancements, including those from dynamic traffic assignment theory, need to be used in educating key managers about the essentials of response and recovery.

Rationale for the Research and Desired Results

Applied research is needed to develop training for incident management and functional recovery. A major effort may be required to prepare information packages and training programs for all operating authorities. Development of the training regimen should incorporate the accepted cycle of identifying requirement analyses (e.g., task, organization, person within each structure), with task-based determination of the associated KSAs, followed by instructional objectives tailored to instill each set of KSAs.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would implement a contract for developing a training program for recovery from an incident involving the transportation infrastructure. Funding required for this effort is estimated to be $1 million. Before 2005, researchers would fully implement the program at an estimated cost of $2 million, and before 2010, continue the training program at an estimated cost of $1 million.

3.4.5 Computer Emergency Response and Emergency Response and Recovery Assessment Capacity Building

Description

Lessons learned from real emergencies, especially those that disrupt the transportation infrastructure, are generally anecdotal and not systematically categorized. Little, if any, formalized economic impact analysis has been performed to determine the

costs and benefits associated with various degrees of emergency preparedness. Trained teams are not available on a continuous or standby basis to collect and disseminate information about (1) the effects of, and mitigation strategies for, computer emergencies or (2) the human factors in responding to an actual emergency and how appropriate measures may be facilitated or hindered by them.

The establishment of a team modeled on, for example, the Computer Emergency Response Team at Carnegie-Mellon University, would provide the needed readiness for the first contingency, while multiple teams, each responsible for a specific geographic region, would deal with the second type. The latter organizations, collectively termed Emergency Response and Recovery Assessment Teams, would conduct interviews, develop chronologies, and generally identify cause and effect and *do's* and *don'ts* in unfolding emergencies. Their ultimate responsibility would be to uncover and formalize the entire body of knowledge of "best practice" in emergency response and recovery actions, especially actions pursuant to attacks on the physical and cyber infrastructure.

Goals and Challenges

Resources, motivation, and efficiency are needed for planning for persons who respond to emergencies. Trained, capable study groups must "stand by" for rapid deployment into the field if a significant emergency occurs.

Rationale for the Research and Desired Results

Applied research is needed to develop an extensive body of knowledge about the best way to accomplish — as well as how *not* to execute — incident management and functional recovery in real time. The outcome would include (1) training tools and programs for emergency responders and (2) identification of technology and coordination needs, with special emphasis on transportation incidents. Development of training must incorporate the accepted cycle of identifying requirement analyses (e.g., task, organization, person within each structure), with task-based determination of the associated KSAs, followed by instructional objectives tailored to instill each set of KSAs.

Timeframe and Resource Requirements

In the near term (before 2002), researchers would define the requirements and procedures needed for developing training materials for emergency responders. Research contracts also would be developed. Funding required for these efforts is estimated to be $3 million. Before 2005, trained teams would be deployed to stand by at strategic locations. Funding required for this effort is estimated at $5 million. Before 2010, and active information exchange would be introduced and procedures would be revised as needed. Funding required for this effort is estimated at $3 million.

3.4.6 Public/Private Infrastructure Security Responsibility

Description

This topic highlights how critical the transportation infrastructure is as a national asset. This importance transcends ownership, which, if true, means that governmental bodies in the United States, especially the federal government, must assume more direct financial and oversight responsibility to assure its security.

Most private operators maintain that they are fully and independently capable of managing their own security, that is, until some hostile incident precipitated by an outside force beyond their control disrupts functionality and, by extension, the movement of goods and people. This issue is predominantly one of policy, but it also requires analysis of jurisdictions and legal structures to clarify (1) command and decision chains for mitigating incidents and (2) management responsibilities in such situations.

Goals and Challenges

In strategic planning, the U.S. Department of Transportation is committed to meeting this objective, and the agency may support research to identify ways to deploy coordinated public and private capabilities in an optimal manner. A unique study approach *may* be required for each control and modal configuration; therefore, six to eight different teams should be involved.

Rationale for the Research and Desired Results

Formalizing of, and agreement to, a set of principles is needed. Doing so would define the foundation on which all structures for enhancing capabilities (in each of the five action areas) would be built.

Timeframe and Resource Requirements

In the near term (before 2002), scoping conferences would be conducted, requests for proposals issued, and project teams selected. Funding required for this effort is estimated to be $2 million. Before 2005, legislation would be proposed (as needed).

Section 4
R&D Topic Roadmaps

This section describes an appropriate roadmap for meeting the 21 research needs identified in Section 3 and summarized in Table D.1. It identifies chronological and complementary links among projects that need to be incorporated into any action plan.

4.1 Vulnerability Analysis of Existing Systems

The goal is to identify (and ultimately mitigate) possibly unrecognized vulnerable pathways in systems with a high degree of centralized command and control and/or open architectures for transmission of electronic information. The objective of applied research is to identify, for up to five typical organization types across transportation operations, significant vulnerabilities that can exist as a function of the communications architecture and control system in place. Research activities should begin as soon as possible after 2002. This topic is interrelated with Topics 2 through 4 and will inform Topics 5, 7, 11, and 16–19. (See figure for explanation of topic numbers, i.e., descriptions.)

4.2 Simulation Tool Development

The goal is to provide a suite of event prediction and management tools that decision makers can use in a gaming framework to (1) shape the construction of preparedness plans for physical and cyber threats, actual attacks, and optimal use of resources; (2) assure continuity of flows in the distribution system; (3) significantly improve the productivity of existing infrastructure; (4) assist in automating decision support systems; and (5) reveal trade-offs among productivity, service reliability, and preparedness for rare events.

The objective of basic and applied research and advanced technology development is to capture and accurately model within the simulation structure all relevant contingencies for each area and mode of transportation, and to enable accurate, detailed modeling of different control hierarchies and the response of system disruptions to these hierarchies. Research activities should be undertaken as soon as practicable, but no later than 2001 because these tools are needed in calendar year 2006; by that time, the United States may be experiencing a “Golden Age” of seamless, multimodal, door-to-door transportation. This topic is interrelated with Topics 1, 3–5, 11, 18, and 19.

4.3 Determination of Risk Perception of Transport System Managers

The goal is to identify and formalize quantitative measures that capture the important characteristics of risk perception at all appropriate decision levels. The objective of basic and applied research is to understand these characteristics across all

modes and to inform researchers that construct simulation and training tools. Research activities should be undertaken as soon as practicable, concurrent with the development of the simulation tools to be available after 2002. This topic precedes Topic 4 and is interrelated with Topics 1, 2, 5, 11, 18, and 19.

4.4 Communication and Inculcation of Sound Risk Management Principles

The primary goal is develop an information and training package about risk, with tools systematically designed for each type and level of control hierarchy. The users are operating authorities in all modes. A second key goal is to institutionalize the principle that daily vulnerability management is a necessary part of normal operation. The objectives of applied technology development are therefore to (1) communicate the nature and magnitude of security risk to decision makers via language and technologies that maximize the transmission of useful, comprehensible information at all appropriate levels; and (2) to prove the principle of vulnerability management in day-to-day practice.

This project would bring relevant aspects of developments in distance learning and training (e.g., via the Internet) into the workplace. Advanced technology development and proof of principle inculcate a physical and cyber security awareness mindset at all levels of operation by tailoring education and training to each worker task, scope of responsibility, and level of education.

Training needs are to be defined and training programs under contract by the end of 2000. Training and support activities are to be under way by the end of 2003, subsequent to development of the simulation described in Topics 1 and 2 and concurrent with, and indirectly related to, activities in Topics 5 and 11. Adoption of principles and practices should begin no later than about 2004. This topic follows Topic 3 and is interrelated with Topics 1, 2, 11, 18, and 19.

4.5 Capacity Margin Analysis

The goal is to develop reliable quantitative estimates of the expected losses from contingencies that arise in the absence of surplus carrying capacity in each component of the transportation system. The objective is to identify an appropriate and necessary level of “surplus” capacity over which federal, state, and/or local governments assume responsibility for maintenance or direct support if they are not economic assets to the owner. Research activities should be undertaken as soon as practicable but will be influenced by the results of research from Topics 1–3; effort could be completed by the end of 2005. This topic is related to Topics 1–4, 11, 18, 19, and 21.

4.6 Emergency Communications

The goal is to identify (and ultimately implement) the secure systems solutions most appropriate for responses to disruptions of transportation infrastructure. The

objective is to provide a head start for product development in the area of fully functional and secure emergency response communications. Research activities are under way, but they should be continued or expanded through 2003. This topic is related to Topics 8, 12, 15, 16, 18, and 19.

4.7 Real-time Hazard, Threat, and Detection Monitoring

The goal is to reduce both unit and deployment costs of detection devices, including those with high-resolution broadband capability. Development for transportation applications is at a relatively early stage in this area. Basic and applied research, followed by advanced technology development and proof of principle and validation, is targeted at preventing physical and cyber intrusion and attack.

Physical (and some cyber) incursions have already occurred, demonstrating the existence of willingness and capability to carry out such incursions. Research and development activities should be undertaken as soon as feasible after 1999, with six to eight parallel analyses being completed by the end of 2005, and public-private partnerships in place (and increasing in number) also by that time. This topic is related to Topics 1, 8, 10, 12–14, 16, and 17.

4.8 Robotics Development and Adaptation

The goal is to identify and develop robotic technologies and remotely controlled servo modules capable of performing the damage assessment duties of first responders without their direct physical intervention. Basic and applied research should be performed to investigate the adaptability of technologies developed and used by DoD and other lead agencies, to identify unmet needs, and to tailor development of the applications to efficient and thorough recovery operations that assist victims and protect responders. A needs assessment and concept development should begin as soon as feasible after 1999; prototype development should be completed by the end of 2005, with public-private partnerships increasing thereafter. This topic is related to Topics 6, 7, 12, 15, 19, and 20.

4.9 Improvement of In-use Performance and Replacement Functionality of Transportation Structures

The goal is to understand the strength and durability of advanced, inexpensive, lightweight materials for permanent and temporary replacement structures that will enable a modularity, portability, and/or durability of function (while meeting high performance standards) generally not available to transportation operations, except in military applications. Basic research should be performed to investigate the adaptability of DoD technologies, identify unmet needs, and apply proof of principle by matching advanced materials with specific structural replacement needs across multiple modes and missions.

Applied research would be conducted to identify and develop materials to meet functional durability needs for maximizing longevity of assets. Needs assessment and

capabilities matching should begin as soon as feasible after 1999, with field tests of competing designs in up to five applications completed by the end of 2005 and commercialization of modular components in place by the end of 2007. This topic is directly related to Topics 5, 10, 19, and 20.

4.10 Unified Vehicle/Guideway Systems (Hardening)

The goal is to enhance resistance to damage from physical and cyber attacks on existing and emerging transportation infrastructures in which the vehicle and guideway constitute integrated systems. The objective of applied research is to identify needs and adapt materials technologies to the systematic improvement of durability in guideway equipment and structures.

Spin-off applications of hardening and other durability improvements to more general types of equipment and structures (e.g., bridges, buildings) are an expected ancillary benefit of this research. Scoping studies should begin in 2000, and research should be under contract to multiple entities by the end of 2001. Comprehensive threat characterization and design of prototypes should be completed by 2008, with field tests, standards definition, commercialization, and some system implementation well under way by 2010. This topic is related to Topics 7, 9, 19, and 20.

4.11 Asset Management

The goal is to define and/or identify reliable quantitative measures to enable each mode and operation to generate plans and programs to use assets that most efficiently use physical and cyber resources. Applied and advanced technology development research address such problems as flaw detection and decision analysis support. The objective is to inculcate globally optimal management principles across all modes.

Requirements should be defined in 2000 and at least two teams awarded development contracts. Database integration and validation testing of a regional/modal prototype set of management tools should be completed by the end of 2005, with direct applications increasing thereafter, at least through 2007. This topic is directly related to Topics 1–5, 9, 10, 12, 14–18, and 21.

4.12 System Representation Improvement

The goal is to maximize the amount of useful data currently available but still in need of transcription into a visual display, that is, collated into clearly comprehensible formats. The objective of advanced technology development and proof of principle and validation for this topic is to improve understanding of interconnected and dependent systems. Knowledge about the structural layouts and strategic organization of such systems is critical for preparing for, and responding to physical and cyber attack.

Requirements should be defined in 2000 and at least two teams awarded development contracts. Database integration and validation testing of a regional prototype set of visual display tools should be completed by the end of 2005, with direct applications increasing thereafter, at least through 2007. This topic is related to Topics 6–8, 13, 14, and 18–20.

4.13 Intrusion Detection

The goal is to upgrade the prevention measures for physical and cyber intrusion and attacks. Because it is believed that the technology and many of the capabilities exist, the objective of advanced technology development and proof of principle and validation for this topic is to adopt and adapt them for action areas in transportation operations, filling in knowledge and performance gaps as completely as possible.

Requirements should be defined in 2000 and development contracts awarded. Design and testing of tools should be completed by the end of 2005, with field implementation thereafter. This topic is related to Topics 7, 12, 14, 16, and 17.

4.14 Cyber Vulnerability Data Warehouse

The goal is to provide access to early warning notification of potential cyber incursion, as well as a real-time channel to the latest information on firewalls and other security practices, to the owners of vulnerable data repositories and networks in the transportation sector. Within a single facility, development teams must craft a combined reference and proactive response capability that meets a wide variety of computer support and security needs across all transportation operations.

Requirements should be defined and development contracts awarded by the end of 2000. The database should be completed and the protocols for access and use of the warehouse should be in place by the end of 2005. This topic is related to Topics 11–13, 15–17, and 19.

4.15 Threat/Intelligence Database and Network

The goal is to craft an efficient, fully integrated facility to develop and disseminate intelligence in regard to specific terrorist plots for destroying physical infrastructure or maliciously “hacking” into transportation functions (computer terrorism). Activities could be modeled on, and directly coordinated with, those of the FBI’s National Infrastructure Protection Center. This topic and Topic 14 (discussed above) could be consolidated if an interagency agreement was in place to create a comprehensive clearinghouse under the aegis of a Transportation Infrastructure Protection Threat Analysis Center. Proof of principle and validation require a broadening and deepening of the scope of existing intelligence networks to embrace all transportation infrastructures.

Requirements should be defined and data development contracts awarded by the end of 2000. The clearinghouse should be fully functional by the end of 2005. This topic is related to Topics 6, 8, 11, and 14.

4.16 Information Assurance

The goal is to identify and implement the most appropriate AI-based technologies for preventing acceptance of unintentionally corrupted or maliciously erroneous electronic information in the various transportation operations. Because the technology and many of the capabilities exist, the objective of applied technology development for this topic is to adopt these capabilities while adapting them to specific needs for message continuity and integrity in transport operations, thereby filling knowledge and performance gaps.

Requirements should be defined and use of existing tools well advanced by the end of 2000. Design and testing should be completed, and tools should be ready for field implementation by the end of 2005, with deployment increasing thereafter. This topic is related to Topics 1, 6, 7, 11, 13, 14, and 17.

4.17 Software Assurance

The goal is to identify and implement the most appropriate AI-based technologies for on-line fault checking and self-diagnosis in critical day-to-day information-handling systems for transportation. Applied technology development is needed to support cyber-incident mitigation.

Requirements should be defined and teams under contract by the end of 2000. Design and testing of customized tools should be completed, and tools should be ready for field implementation by the end of 2005. This topic is related to Topics 1, 6, 7, 11, 13, 14, and 16.

4.18 Human Factors Analysis

The goal is to characterize the problems and limitations in event preparedness, prediction, and response that are specifically attributable to the human role in the operation and maintenance of transportation systems. In particular, applied research is needed to identify and quantify these problems and limitations in vulnerability assessment, incident mitigation, and incident management. The objective is to develop information packages and training programs applicable to a wide range of operations and authorities.

Requirements should be defined and teams under contract by the end of 2000. New and modified procedures, tools, and control systems should be in the demonstration and training phases by the end of 2005. This topic is related to Topics 1–5, 11, 12, 19, and 20.

4.19 Recovery Training

The goal is to bring many methodological advancements, including those from dynamic traffic assignment theory, to educate key managers at all relevant levels about the essential components of response and recovery as appropriate to their respective and collective operations. The goal of applied research into training needs for incident management and functional recovery training would be to develop packages that would maximize communication to, and endorsement by, all operating authorities. Training needs should be defined and training programs should be under contract by the end of 2000. Training should take place across all operations no later than 2005. This topic is related to Topics 1–6, 8–10, 12, 14, 18, and 20.

4.20 Computer Emergency Response and Emergency Response and Recovery Assessment Capacity Building

The goal is to develop and formalize an extensive body of knowledge about the best way to accomplish — and, conversely, how *not* to execute — incident management and functional recovery in real time. The recommended applied research method involves maintaining trained, capable study groups in "stand-by" mode for rapid deployment into the field if a significant emergency occurs. This practice would enable systematic recording and documentation of specific actions and events or dissemination of necessary information. The objective of the research is to develop training programs for emergency responders, with special emphasis on transportation infrastructures and incidents.

Data needs and collection procedures should be defined and training programs should be under contract by the end of 2000. Sets of trained teams would then be deployed in stand-by mode for two to four years thereafter, with information and training dispersal occurring widely across all operations no later than 2008. This topic is related to Topics 8–10 and 12–14.

4.21 Public/Private Infrastructure Security Responsibility

The goal is to formalize an agreed-upon set of principles that define the foundation and governing of the mechanisms for enhancing capabilities to protect physical and cyber components of the transportation infrastructure. The objective is to analyze jurisdictions and legal structures to clarify command and decision chains for incident mitigation and situation management. Proof of principle and validation would focus on optimal deployment of public and private capabilities for mutual reinforcement across all relevant control structures and modal operations.

Scoping conferences should be conducted, and six to eight research teams should be selected in 2000, with research recommendations submitted in 2002 and any necessary legislation proposed no later than 2005. This topic is related directly to Topics 5 and 11, but it crosscuts all action areas and therefore is indirectly related to all topics.

4.22 Crosswalks and Milestones

Figure D.1 classifies the topics by action area and interrelationships. Each R&D topic is assigned a row and/or column. By reading across each row or down each column, it is possible to see how that a specific topic area is related to other topic areas in one or more of the five action areas (Section 2). For example, R&D Topic 1, Vulnerability Analysis of Existing Systems (column 1), is related to Simulation Tool Development, Determination of Risk Perception of Transport System Managers, and Communication and Inculcation of Sound Risk Management Principles through the Awareness Training action area.

Further, Topic 1 is related to Capacity Margin Analysis through the Incident Mitigation and Incident Management areas; to Real-Time Hazards, Threat, and Detection Monitoring, Information Assurance, and Software Assurance through Intrusion and Attack Prevention and Incident Management; to Human Factors Analysis through Awareness, Mitigation, and Management (three areas); and to Recovery Training through Incident Management and Functional Recovery. This topics relationships to Asset Management and Public/Private Responsibility cut across all action areas.

Table D.2 shows the milestones that the study team agreed on as being achievable for each R&D topic up to 2010.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
2	**A**																				
3	**A**	**A**																			
4	**A**	**A**	**A**																		
5	**Mi,Ma**	**Mi,Ma**	**Mi,Ma**	**Mi,Ma**																	
6																					
7	**P, Ma**																				
8						**Ma, R**	**P**														
9					**P, Ma**																
10							**P, Mi**		**Mi, R**												
11	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**											
12						**Mi,Ma**	**P, Mi,Ma**	**Ma**			**X**										
13							**P**				**X**	**P, Mi**									
14											**X**	**P, Mi**	**P, Mi**								
15						**P, Mi,Ma**		**Ma, R**			**X**			**P, Mi**							
16	**P, Ma**					**Mi**	**P, Mi**				**X**		**P, Mi**	**P, Mi**							
17	**P, Ma**					**P, Mi**	**P, Mi**				**X**		**P, Mi**	**P, Mi**		**P, Mi**					
18	**A,Mi, Ma**	**A,Mi, Ma**	**A,Mi, Ma**	**A,Mi, Ma**	**A,Mi, Ma**	**A,Mi, Ma**					**X**	**A,Mi, Ma**									
19	**Ma, R**	**Ma, R**	**Ma, R**	**Ma, R**	**Mi,Ma R**	**Ma, R**		**Ma, R**	**Ma, R**	**Ma, R**	**X**	**Ma, R**		**Ma, R**				**Ma, R**			
20								**Ma, R**	**Ma, R**	**Ma, R**	**X**	**Ma, R**						**Ma, R**	**Ma, R**		
21	**X**	**X**	**X**	**X**	**X : Mi,Ma**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	

A = Awareness training
P = Intrusion and attack prevention
Mi = Incident mitigation
Ma = Incident management
R = Functional recovery
X = Crosses all action areas

Figure D.1 Topical Interrelationships by Action Area[a]

[a]Numbering Key for Figure D.1

No.	Description of R&D Topic
1	Vulnerability Analysis of Existing Systems
2	Simulation Tool Development
3	Determination of Risk Perception of Transport System Managers
4	Communication and Inculcation of Sound Risk Management Principles
5	Capacity Margin Analysis
6	Emergency Communications
7	Real-time Hazard, Threat, and Detection Monitoring
8	Robotics Development and Adaptation
9	Improvement of In-use Performance and Replacement Functionality of Transportation Structures
10	Unified Vehicle/Guideway Systems (Hardening)
11	Asset Management
12	System Representation Improvement
13	Intrusion Detection
14	Cyber Vulnerability Data Warehouse
15	Threat/Intelligence Database and Network
16	Information Assurance
17	Software Assurance
18	Human Factors Analysis
19	Recovery Training
20	Computer Emergency Response and Emergency Response and Recovery Assessment Capacity Building
21	Public/Private Infrastructure Security Responsibility

Table D.2 Summary of Transportation R&D Roadmap

R&D Topic No.	Title	Near Term (Resource Estimate[a])	Achieved by ~2005 (Resource Estimate[a])	Achieved by ~2010 (Resource Estimate[a])
1	Vulnerability Analysis of Existing Systems	Conduct pilot studies of actual operations. ($9 million)	Develop assessment tools. ($9 million)	Complete assessments of transportation systems. ($6 million)
2	Simulation Tool Development	Identify and evaluate ways to create tools that can be used in event prediction and management. ($15 million)	Develop and validate basic tools. ($15 million)	Validate and deploy completed model suite. ($5 million)
3	Determination of Risk Perception of Transport System Managers	Conduct scoping. ($2 million)	Complete analyses. ($1 million)	Update as required.
4	Communication and Inculcation of Sound Risk Management Principles	Develop training program. ($2 million)	Complete analyses and have training actively occurring in all operating functions. ($2 million)	Identify and implement fully secure emergency response communications.
5	Capacity Margin Analysis	Sign contract for analytical team(s). (>$1 million)	Complete analytical effort. (>$1 million)	
6	Emergency Communications	Identify and implement fully secure emergency response communications. ($6 million)	Commercialize high-reliability, secure emergency response communications. ($2 million)	
7	Real-time Hazard, Threat, and Detection Monitoring	Ensure applied R&D is under contract. Develop detection devices. ($8 million)	Complete prototype testing. ($12 million)	Commercialize public-private ventures. ($12 million)
8	Robotics Development and Adaptation	Develop and adapt robotic, remotely controlled modules. ($5 million)	Complete prototype testing. ($7 million)	Commercialize public/private ventures.
9	Improvement of In-use Performance and Replacement Functionality of Transportation Structures	Develop and adapt materials to maximize modularity, portability, and/or durability. ($5 million)	Complete field testing in up to five applications. ($7 million)	Commercialize structures.
10	Unified Vehicle/Guideway Systems Hardening	Complete scoping studies of materials technologies. ($2 million)	Develop prototypes to improve durability of transport systems. ($2 million)	Perform field testing, and define and implement standards. ($2 million)
11	Asset Management	Conduct scoping. ($1 million)	Validate and peer-review prototype tools. ($2 million)	Commercialize tools. ($1 million)
12	System Representation Improvement	Develop contracts with at least two teams. Improve methods to manage transport system data in a clear format. ($20 million)	Integrate database. Complete prototype tools. ($30 million)	Implement multiple applications. ($20 million) (full U.S. coverage assumed)

Table D.2 (Cont.)

R&D Topic No.	Title	Near Term (Resource Estimate[a])	Achieved by ~2005 (Resource Estimate[a])	Achieved by ~2010 (Resource Estimate[a])
13	Intrusion Detection	Define requirements and award contracts to customize intrusion detection systems. ($4 million)	Complete design and testing of systems. Begin to implement multiple applications. ($6 million)	Commercialize intrusion detection for physical and cyber assets. ($1 million)
14	Cyber Vulnerability Data Warehouse	Define requirements and award contracts. ($1 million)	Complete and verify database. Warehouse access protocol. ($2 million)	
15	Threat/Intelligence Database and Network	Define requirements and award contracts for an integrated facility for providing intelligence concerning threats. ($1 million)	Complete a fully functional facility. ($2 million)	
16	Information Assurance	Define requirements and use existing tools to develop AI-based technologies. ($2 million)	Complete design and testing of new tools. ($3 million)	Implement and commercialize AI-based technologies. ($1 million)
17	Software Assurance	Identify requirements for on-line fault checking in information systems. ($4 million)	Complete design and testing of new tools in critical information systems. ($6 million)	Complete field implementation and commercialization. ($1 million)
18	Human Factors Analysis	Characterize problems and limitations inherent in preparedness, prediction, and response. Award contract. ($6 million)	Fully identify and implement changes for preparedness/prediction. ($4 million)	
19	Recovery Training	Contract for training program development. ($1 million)	Implement training program. ($2 million)	Continue training program. ($1 million)
20	Computer Emergency Response and Emergency Response and Recovery Assessment Capacity Building	Define needs and procedures. Develop research contracts. ($3 million)	Deploy trained teams to standby mode at strategic locations. ($5 million)	Introduce active information exchange and revise procedures as needed. ($3 million)
21	Public/Private Infrastructure Security Responsibility	Conduct scoping conferences. Issue requests for proposals. Select project teams. ($2 million)	Propose legislation (as needed).	

[a] Resource estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

Note

Several areas of substantive disagreement surfaced in reviewer comments on earlier drafts of this report. These areas, and the responses by the team, are provided below.

1. **Risk management and risk evaluation in transportation operations are well-established, private-sector management practices that require no additional research.** Some reviewers expressed dissatisfaction with the roadmap's implicit premise that private-sector managers and decision makers need additional education and training in risk management for physical and cyber vulnerabilities. They expected those officials to be insulted and possibly angered by the presumption that any "expert" from outside their industry could add useful information.

   There is little doubt that, without early and direct interaction with such managers through, for example, a pilot study to discover the actual extent of their information needs, the ultimate findings of any risk management research would have little value because such findings would be ignored by the very audience to which they are directed. This is why the roadmap emphasizes and reemphasizes the importance of early management involvement and "buy-in" for many of the projects described.

   In general, the team confirmed, after speaking with several private-sector management representatives, that officials are looking for better information on which to base their strategic security decisions, especially in cyber vulnerability. Moreover, the recent, major, and protracted disruptions in commodity flow on the domestic rail system argue that the presumed resiliency of the line haul transportation system is not as complete as some would hold. Such critical system performance failures under *normal* operating practice do not bode well for a swift and wholly satisfactory system recovery from major physical or cyber attacks.

2. **The roadmap does not give sufficient attention to air transport security needs.** The team does not dispute that the roadmap's list of recommended projects contains few projects *specifically* targeted at air transportation, although many are as relevant to aviation as to other transportation modes. To avoid redundancy and duplication of effort, the team has deferred to (and incorporated by reference) the programs and projects outlined in the FAA's Security Research and Development Program developed pursuant to the Final Report of the White House Commission on Aviation Safety and Security.

3. **A critical path diagram is needed.** A critical path diagram implies that a functionally inseparable fixed chronology and chain of dependencies are necessary to

accomplish the desired set of goals. The team uniformly agrees that such fixed dependencies do not exist for the research program outlined. Although certain activities clearly must precede others (for example, fact-finding, documentation, and formalization of procedures before training begins), none of the actual *research* needed is contingent on the completion of other research in the roadmap. Additional discovery, updating, and refinement of results can occur in parallel or in tandem across virtually the entire project slate. In a sense, this action was deliberate on the part of the team, which individually and collectively believes that all research is equally valid and could produce useful results almost immediately. Thus, no research effort should be hindered or vitiated because it is chronologically "downstream" of other work that may not be progressing satisfactorily.